

Recipes to Fermat-type equations of the form

$$x^r + y^r = Cz^p$$

Nuno Freitas

February 27, 2013

Abstract

In this paper we discuss a general approach to Diophantine equations of the form $x^r + y^r = Cz^p$ via Hilbert modular forms over some totally real subfields of $\mathbb{Q}(\zeta_r)$. In particular, we will prove for $r = 7$ the non-existence of primitive solutions (a, b, c) such that $7 \nmid c$ and give explicit Frey-curves for $r = 11, 13, 17, 19$. Furthermore, for primes $r = 4m + 1$ we will give an extra method to construct two more Frey-curves.

1 Introduction

After the proof of Fermat's Last Theorem by Wiles [27] mathematicians have been generalizing the initial strategy of Frey, Hellegouarch, Serre, Ribet and Wiles that lead to the solution of FLT and trying to solve more Diophantine equations. The most important unsolved family of equations which directly relates to the *ABC*-conjecture is the generalized equation of form

$$Ax^p + By^q = Cz^r \quad \text{where} \quad 1/p + 1/q + 1/r < 1.$$

As a consequence of the work of Darmon-Granville [8]) it is known that for a fixed triple (p, q, r) there exists only a finite number of solutions to the equation above such that $(x, y, z) = 1$ (called primitive solutions). However, the total number of primitive solutions is expected to be finite for all possible triples (p, q, r) . As evidence for these, many particular cases of the generalized equation were solved, including infinite families. A remarkable subfamily for which there have been developments is the generalized Fermat equation $x^p + y^q = z^r$. In the introduction of [5] there is a survey of results on this equations.

Another important subfamily are the equations of signature (r, r, p) , that is, $Ax^r + By^r = Cz^p$ with r a fixed prime. Into this direction there is work for $(3, 3, p)$ by Kraus [19], Bruin [4], Chen-Siksek [6] and Dahmen [7]; for $(5, 5, p)$ by Billerey [2], Billerey-Dieulefait [3] and Dieulefait-Freitas [10]; for $(13, 13, p)$ from the author joint with Dieulefait [9].

In this paper we describe a general strategy to go further into the study of equations of type (r, r, p) . More precisely, for a fixed $r > 5$ our method will allow us to attack equations with shape

$$x^r + y^r = Cz^p, \tag{1}$$

for C in an infinite family of integers only divisible by primes $q \not\equiv 1, 0 \pmod{r}$. Let (a, b, c) be a triple of integers such that $a^r + b^r = Cc^p$. We say that it is

a *primitive* solution if $(a, b) = 1$ and we will say that it is a *trivial* solution if $abc = 0$. Following the terminology introduced by Sophie Germain in her work on the FLT we will divide solutions to (1) into two cases

Definition 1.1 *A primitive solution (a, b, c) of $x^r + y^r = Cz^p$ is called a first case solution if r do not divide c , and a second case solution otherwise.*

As it will be explained the method presented here can only succeed in proving the non-existence of primitive first case solutions. It goes as follows: we first relate a non-trivial primitive solution (a, b, c) of (1) to a non-trivial primitive solution (a, b, c_1) of another Diophantine equation with coefficients in K^+ (the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_r)$) with the extra condition $C \mid a + b$. Then we attach to the solution (a, b, c_1) a Frey-curve $E_{(a,b)}$ defined over K^+ which is not a \mathbb{Q} -curve. We prove the absolutely irreducibility of $\bar{\rho}_{E,p}$ (the mod p residual representation attached to E) for p greater than a constant. Then if the Frey-curves $E_{(a,b)}$ are supposed modular (in some cases we can prove they actually are) we are able to apply the lowering the level results for Hilbert modular forms over K^+ to get the congruence $\rho_{E,p} \equiv \rho_{f,p} \pmod{\mathfrak{P}}$, where f is a Hilbert newform of a convenient level. To finish the proof and conclude that (a, b, c) can not exist we have use the values $a_q(E)$, the fact that $C \mid a + b$ and $r \nmid c$ (first case solution) to contradict the congruence.

In general, our strategy will find computational difficulties. The problem being that the degree of K^+ is $(r-1)/2$, which grows with r , and consequently the dimension of the cusp spaces that we need to consider will grow extremely fast. Actually, already for small values of r we will find impossible computations. Nevertheless, if $r \equiv 1 \pmod{6}$ we will show that Frey-curves over a subfield K_0 of K^+ exists. In this case K^+ has degree $3k$, K_0 will have degree k and this difference is enough for the computation of newforms to be possible for a few r . In particular, for $r = 13$ the strategy described here is applied in [9], where modularity of the Frey-curves is proved and the existence of first case solutions completely demonstrated.

In this work, along with the general method, we will also take advantage of this computational difference and prove the non existence of first case solutions for $r = 7$ (see Theorem 3.1). And as a collateral result of that proof we will also solve an equation of the form $\phi(x, y) = 71z^p$, where $\phi(x, y)$ is a degree 6 homogeneous polynomial (see Theorem 3.3). We will also give explicit Frey-curves for a few small values of r . Moreover, in the last section using a different strategy we will construct two more Frey-curves for when r is of the form $4m+1$.

2 The recipe for $x^r + y^r = Cz^p$

Let C be an integer only divisible by primes $q \not\equiv 1, 0 \pmod{r}$. In this section we describe a general strategy to study equations of the form

$$x^r + y^r = Cz^p \tag{2}$$

where $r > 5$ is a fixed prime. Since the factorization

$$x^r + y^r = (x + y)\phi_r(x, y)$$

will be key to our method we start by proving a few properties about $\phi_r(x, y)$.

2.1 Properties of $\phi_r(x, y)$

Let ζ denote a r -root of unity. Observe that

$$\phi_r(x, y) = \prod_{i=0}^{r-1} (-1)^i x^{r-1-i} y^i.$$

and consider the decomposition over the cyclotomic field $\mathbb{Q}(\zeta)$

$$\phi_r(x, y) = \prod_{i=1}^{r-1} (x + \zeta^i y). \quad (3)$$

Proposition 2.1 *Let \mathfrak{P}_r be the prime in $\mathbb{Q}(\zeta)$ above the rational prime r and suppose that $(a, b) = 1$. Then, any two different factors $a + \zeta^i b$ and $a + \zeta^j b$ in the factorization of $\phi_r(a, b)$ are coprime outside \mathfrak{P}_r . Furthermore, if $r \mid a + b$ then $\nu_{\mathfrak{P}_r}(a + \zeta^i b) = 1$ for all i .*

Proof: Suppose that $(a, b) = 1$. Let \mathfrak{P} be a prime in $\mathbb{Q}(\zeta)$ above $p \in \mathbb{Q}$ and a common prime factor of $a + \zeta^i b$ and $a + \zeta^j b$, with $i > j$. Observe that $(a + \zeta^i b) - (a + \zeta^j b) = b\zeta^j(1 - \zeta^{i-j}) \in \mathfrak{P}$. Since \mathfrak{P} can not divide b because in this case it would also divide a we conclude that $\zeta^i(1 - \zeta^{i-j}) \in \mathfrak{P}$ but ζ^i is a unit so $1 - \zeta^{i-j} \in \mathfrak{P}$, that is $\mathfrak{P} = \mathfrak{P}_r$. Now for the last statement in the proposition, suppose that $r \mid a + b$. Then,

$$a + \zeta^i b = a + b - b + \zeta^i b = (a + b) + (\zeta^i - 1)b,$$

and since $\nu_{\mathfrak{P}_r}(\zeta^i - 1) = 1$ we have $\nu_{\mathfrak{P}_r}(a + \zeta^i b) = \min\{r - 1, 1\} = 1$ ■

Corollary 2.2 *If $(a, b) = 1$, then $a + b$ and $\phi_r(a, b)$ are coprime outside r . Furthermore, if $r \mid a + b$ then $\nu_r(\phi_r(a, b)) = 1$.*

Proof: Let p be a prime dividing $a + b$ and $\phi_r(a, b)$ and denote by \mathfrak{P} a prime in $\mathbb{Q}(\zeta)$ above p . \mathfrak{P} must divide at least one of the factors $a + \zeta^i b$. Since a, b are integers \mathfrak{P} can not divide b then it follows from

$$a + b = a + \zeta^i b - \zeta^i b + b = (a + \zeta^i b) + (1 - \zeta^i)b$$

that $\mathfrak{P} = \mathfrak{P}_r$. Moreover, if $r \mid a + b$ it follows from the proposition that $\nu_{\mathfrak{P}_r}(a + \zeta^i b) = 1$ for all i then $\nu_{\mathfrak{P}_r}(\phi_r(a, b)) = r - 1$ thus $\nu_r(\phi_r(a, b)) = 1$. ■

Proposition 2.3 *Let $(a, b) = 1$ and $l \not\equiv 1 \pmod{r}$ be a prime dividing $a^r + b^r$. Then $l \mid a + b$.*

Proof: Since l divides $a^r + b^r$, $l \nmid ab$. Let b_0 be the inverse of $-b$ modulo l . We have $a^r \equiv (-b)^r \pmod{l}$, hence $(ab_0)^r \equiv 1 \pmod{l}$. Thus the multiplicative order of ab_0 in \mathbb{F}_l is 1 or r . From the congruence $ab_0 \equiv 1 \pmod{l}$ it follows $a + b \equiv 0 \pmod{l}$. If $l \nmid a + b$ then the order of ab_0 is r and $l \equiv 1 \pmod{r}$. ■

2.2 Relating two Diophantine equations.

Recall that $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ is the maximal totally real subfield of $\mathbb{Q}(\zeta)$ and let h_r^+ be its class number. Let π_r be such that $r\mathcal{O}_{K^+} = (\pi_r)^{(r-1)/2}$ and denote ϕ_r only by ϕ . Suppose that there exists a non-trivial primitive solution (a, b, c) to (2), then it follows from Corollary 2.2 and Proposition 2.3 that there exists a non-trivial primitive solution (a, b, c_0) to

$$\phi(a, b) = c_0^p, \quad (4)$$

with $C \mid a + b$ and $r \nmid a + b$ or to

$$\phi(a, b) = rc_0^p \quad (5)$$

with $C \mid a + b$ and $r \mid a + b$, where in both cases c_0 is only divisible by primes congruent to 1 modulo r .

Since $r - 1 \geq 6$ is even we can pick three different degree two factors of ϕ of the form $f_i = (x + \zeta^{k_i}y)(x + \zeta^{r-k_i}y)$ with coefficients in K^+ . Given a primitive solution (a, b, c_0) of equation (4) or (5) we have $(a, b) = 1$ and by Proposition 2.1 we know that the $f_i(a, b)$ are pairwise coprimes outside \mathfrak{P}_r . Then since \mathcal{O}_{K^+} is a Dedekind domain we have that $(f_i(a, b)) = \mathcal{I}^p$ or $(f_i(a, b)) = (\pi_r)\mathcal{I}^p$ as ideals in \mathcal{O}_{K^+} . These identities show that the order of \mathcal{I} in the ideal class group of K^+ divides p . Thus if we suppose that $p > h_r^+$ we have that \mathcal{I} is principal and we can write $f_i(a, b) = \mu_i c_i^p$ or $f_i(a, b) = \mu_i \pi_r c_i^p$, where $\mu_i, c_i \in \mathcal{O}_{K^+}$ with μ_i an unit. Thus as long as $p > h_r^+$ we have transformed the solution (a, b, c_0) into a solution (a, b, c_1) (with c_1 an integer in K^+) of the equation (with coefficients in K^+)

$$f_1(a, b)f_2(a, b)f_3(a, b) = \mu c_1^p \quad (6)$$

or

$$f_1(a, b)f_2(a, b)f_3(a, b) = \mu \pi_r^3 c_1^p, \quad (7)$$

respectively, where $\mu \in K^+$ is some unit. Moreover, $C \mid a + b$ in both cases, $r \nmid a + b$ in (6) and $r \mid a + b$ in (7).

To summarize: for $p > h_r^+$ we have related an integer non-trivial primitive solution (a, b, c) to (2) to a non-trivial primitive solution $(a, b, c_1) \in \mathbb{Z}^2 \times \mathcal{O}_K$ of an equation with coefficients in K^+ with extra hypothesis on the divisors of $a + b$. From now on we will study these latter solutions using the modular approach via Hilbert modular forms.

2.3 The Frey-Hellegouarch curves

We now want to attach a Frey-Hellegouarch curve to a putative non-trivial primitive solution $(a, b, c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ to (6) or (7). Let f_i be the degree two factors of ϕ with coefficients in K^+ mentioned in the previous section, that is

$$\begin{cases} f_1(x, y) = x^2 + (\zeta^{k_1} + \zeta^{r-k_1})xy + y^2, \\ f_2(x, y) = x^2 + (\zeta^{k_2} + \zeta^{r-k_2})xy + y^2, \\ f_3(x, y) = x^2 + (\zeta^{k_3} + \zeta^{r-k_3})xy + y^2. \end{cases}$$

Hence, if we find a triple (α, β, γ) such that

$$\alpha f_1 + \beta f_2 + \gamma f_3 = 0,$$

we can define $A(a, b) = \alpha f_1(a, b)$, $B(a, b) = \beta f_2(a, b)$, $C(a, b) = \gamma f_3(a, b)$ and consider the Frey-curves with classic form

$$E_{(a,b)} : y^2 = x(x - A(a, b))(x + B(a, b)),$$

attached to a non-trivial primitive integer solution (a, b, c) of (6) or (7). Observe from the form of the f_i that finding the desired triple is always possible, because it is a solution of a linear system with two equations and 3 variables. In particular, we choose the solution

$$\begin{cases} \alpha = -(\zeta^{k_2} + \zeta^{r-k_2} - \zeta^{k_3} - \zeta^{r-k_3}), \\ \beta = \zeta^{k_1} + \zeta^{r-k_1} - \zeta^{k_3} - \zeta^{r-k_3}, \\ \gamma = -\zeta^{k_1} - \zeta^{r-k_1} + \zeta^{k_2} + \zeta^{r-k_2}. \end{cases}$$

Furthermore, to the curves $E_{(a,b)}$ are associated the following quantities:

$$\begin{aligned} \Delta(E) &= 2^4(ABC)^2, \\ c_4(E) &= 2^4(AB + BC + AC), \\ c_6(E) &= -2^5(C + 2B)(A + 2B)(2A + B), \\ j(E) &= 2^8 \frac{(AB + BC + AC)^3}{(ABC)^2}. \end{aligned}$$

In particular,

$$\Delta(E) = \begin{cases} \mu^2 2^4 (\alpha\beta\gamma)^2 c^{2p} & \text{if } r \nmid a+b, \\ \mu^2 2^4 (\alpha\beta\gamma)^2 \pi_r^6 c^{2p} & \text{if } r \mid a+b. \end{cases}$$

As expected, c appears to a p -power in the discriminant which is fundamental for the modular approach to work.

Let \mathfrak{P} , \mathfrak{P}_r and \mathfrak{P}_2 denote a prime in K^+ above p , r and 2, respectively. Denote by $\text{rad}(c)$ the product of the primes dividing c .

Proposition 2.4 *Suppose that $(a, b) = 1$. The conductor of the curves $E_{(a,b)}$ is of the form*

$$N_E = 2^s \mathfrak{P}_r^t \text{rad}(c),$$

where s may be 2, 3 or 4 and $t = 0$ or 2 if $r \mid a+b$ or $r \nmid a+b$, respectively.

Proof: To the results used in this proof we follow [21]. First note that α, β, γ can be written in the form $\pm \zeta^s (1 - \zeta^t)(1 - \zeta^u)$ which means that the only prime dividing $\alpha\beta\gamma$ is \mathfrak{P}_r and $v_{\mathfrak{P}_r}(\alpha\beta\gamma) = 3$.

Let \mathfrak{P} be a prime in K^+ different from \mathfrak{P}_r and \mathfrak{P}_2 . Observe that $v_{\mathfrak{P}}(\Delta(E)) = 2pv_{\mathfrak{P}}(c)$. Then if $\mathfrak{P} \nmid c$ we have $v_{\mathfrak{P}}(\Delta) = 0$ and the curve has good reduction. If $\mathfrak{P} \mid c$ then $v_{\mathfrak{P}}(\Delta) > 0$ and \mathfrak{P} must divide only one among A, B or C (see Proposition 2.1). From the form of c_4 it can be seen that $v_{\mathfrak{P}}(c_4) = 0$ thus E has multiplicative reduction at \mathfrak{P} .

Since $(\pi_r) = \mathfrak{P}_r$ we see from the form of $\Delta(E)$ that $v_{\mathfrak{P}_r}(\Delta) = 6$ or 12 if $r \nmid a+b$ or $r \mid a+b$, respectively. This translate to E bad additive reduction ($v_{\mathfrak{P}_r}(N_E) = 2$) or good reduction ($v_{\mathfrak{P}_r}(N_E) = 0$) at \mathfrak{P}_r if $r \nmid a+b$ or $r \mid a+b$, respectively.

Since 2 do not ramifies in $\mathbb{Q}(\zeta)$ we use Table IV in [21]. It is easily seen by from the shape of Δ , c_4 and c_6 that $v_{\mathfrak{P}_2}(\Delta) = 4$, $v_{\mathfrak{P}_2}(c_6) = 5$ and $v_{\mathfrak{P}_2}(c_4) \geq 4$

for any \mathfrak{P}_2 above 2. Then the equation is minimal ($v_{\mathfrak{P}_2}(\Delta) < 12$) and we check in Table IV [21] for the columns corresponding to the previous valuations and observe that $v_{\mathfrak{P}_2}(N_E)$ can be 2, 3, 4 corresponding to Kodaira type II, III or IV. ■

In the next section we will prove the next theorem and comment on the conjecture bellow, but by now we will suppose both to be true.

Theorem 2.5 *Let $\bar{\rho}_{E,p}$ be the mod p Galois representation attached to E . There exists a constant $M(r)$ such that if $p > M(r)$ then the representation $\bar{\rho}_{E,p}$ is absolutely irreducible.*

Conjecture 2.6 *The curves $E_{(a,b)}$ over K^+ are modular.*

For an ideal N of K^+ we denote by $S_2(N)$ the set of Hilbert modular cusp forms of parallel weight 2 and level N . It follows from modularity that there exists a newform f_0 in $S_2(2^i \mathfrak{P}_r^t \text{rad}(c))$ such that $\rho_{E,p}$ is isomorphic to the p -adic representation associated with f_0 , which we denote by $\rho_{f_0,p}$. In this situation, for $p > M(r)$ we want to apply the lowering the level results for Hilbert modular forms from Jarvis, Rajaei and Fujiwara. We first determine the Artin conductor $N(\bar{\rho}_{E,p})$. Recall that $p \neq r$ hence it is unramified in K^+ . Let l be a semistable prime of E , i.e. those dividing c . If $l \neq p$ since it appears to a p -th power in the discriminant $\Delta(E)$ we know by an argument of Hellegouarch that the representation $\bar{\rho}_{E,p}$ will not ramify at these primes. Furthermore, when reducing to the residual representation the conductor at the bad additive primes can not decrease hence $N(\bar{\rho}_{E,p}) = 2^i \mathfrak{P}_r^t$.

Since $\bar{\rho}_{E,p}$ is modular and irreducible we now apply results on level lowering. Since K^+ might be of even degree, in order to apply the main result of [25], we need to add to the level an auxiliary prime. The auxiliary prime \mathfrak{q} , in particular, satisfies that $\bar{\rho}_{f_0,p}(\text{Frob}_{\mathfrak{q}})$ is conjugated to $\bar{\rho}_{f_0,p}(\sigma)$, where σ is complex conjugation. We now apply the main theorem in [25] to remove from the level all primes except those above 2, p , the prime \mathfrak{P}_r and \mathfrak{q} . Now we will remove from the level the primes above p and for that we need $\bar{\rho}_{E,p}|G_{\mathfrak{P}}$ to be finite at all primes $\mathfrak{P} \mid p$. If $\mathfrak{P} \nmid c$ is of good reduction then $\bar{\rho}_{E,p}|G_{\mathfrak{P}}$ is finite; if $\mathfrak{P} \mid c$ is of multiplicative reduction, since we have $p \mid v_{\mathfrak{P}}(\Delta)$ it is known that $\bar{\rho}_{E,p}|G_{\mathfrak{P}}$ is finite. Thus from Theorem 6.2 in [13] we can remove the primes above p without changing the weight. Finally, from the condition imposed on \mathfrak{q} follows that $\text{Nm}(\mathfrak{q}) \not\equiv 1 \pmod{p}$ and we can apply Fujiwara version of Mazur's principle to remove \mathfrak{q} from the level. Then we conclude that there exists a newform f in $S_2(2^i \mathfrak{P}_r^t)$ such that its associated mod p Galois representation satisfies

$$\rho_{E,p} \equiv \rho_{f_0,p} \equiv \rho_{f,p} \pmod{\mathfrak{P}}. \quad (8)$$

Then if we show that this congruence can not hold for all the newforms in the corresponding cusp spaces $S_2(2^i \mathfrak{P}_r^t)$ we have proved that our putative solution (a, b, c) can not exist hence (2) also can not have non-trivial primitive solutions. The most common method to contradict the previous congruence is to look at the values $a_q(E)$ and $a_q(f)$ and verify that they can not be congruent modulo \mathfrak{P} if p is greater than a constant. However, this method is limited by the existence of trivial solutions.

An intrinsic problem of these curves is that for some μ the equations (6) and (7) have trivial solutions $\pm(1, 0, 1)$, $\pm(0, 1, 1)$, $(1, 1, 1)$ and $(1, -1, 1)$, $(-1, 1, 1)$

that are associated with the Frey-curves $E_{(1,0)}$, $E_{(1,1)}$ and $E_{(1,-1)}$, respectively, which are indeed elliptic curves. Then we will not be able to eliminate their (conjecturally) associated newforms simply by comparing the values of a_q . However, for suitable values of C the extra condition $C \mid a + b$ should be enough to deal with $E_{(1,0)}$ and $E_{(1,1)}$, but the curve $E_{(1,-1)}$ will survive. To eliminate the newform corresponding to $E_{(1,-1)}$ we need the extra hypothesis $r \nmid a + b$ to achieve a contradiction at the inertia at \mathfrak{P}_r . From Proposition 2.3 it follows that for a primitive solution (a, b, c) of (2) we have $r \nmid a + b \Leftrightarrow r \nmid c$ thus we are limited to solve the equation (2) only for first case solutions (see Definition 1.1).

Remark 2.7 *Our method can be adapted to solve some equations completely, i.e the restriction $r \nmid c$ on the solutions may be removed. This is the case if instead we consider the equation $x^{2r} + y^{2r} = Cz^p$, in which case we use the Frey-curves $F_{(a,b)} := E_{(a^2, b^2)}$. Since the trivial solutions $(1, -1)$ will correspond to the curve $F_{(1,-1)} = E_{(1,1)}$ which in principle can be eliminated because of the condition $C \mid a + b$. This will be illustrated in section 3 for $r = 7$.*

There are also obvious computational limitations to the strategy, because the dimension of K^+ is $(r - 1)/2$ and increases with r . In particular, the norm of 2 and \mathfrak{P}_r increase and consequently also the norm of the conductor of $E_{(a,b)}$ increases making the dimension of the corresponding space of Hilbert modular cuspforms increase fast. For example, when $r = 11$ the norm of $2^4\mathfrak{P}_r^2$ is $2^{20}11^2$ and the dimension of $S_2(2^4\mathfrak{P}_r^2)$ is 5406721. Thus, already for small values of r computing the corresponding newspace of Hilbert modular forms of $S_2(2^4\mathfrak{P}_r^2)$ is infeasible.

However, if $r \equiv 1 \pmod{6}$ the computational requirements can be reduced. Indeed, the degree of ϕ is of the form $6k$ then we can find k factors of ϕ (ϕ_i for $1 \leq i \leq k$) with degree six and coefficients in the totally real subfield of K^+ with degree k (denote it by K_0). Let σ be the generator of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and let ϕ_1 be the factor of ϕ_r given by

$$\phi_1 = \prod_{i=0}^5 (x + \sigma^{ik}(\zeta)y)$$

and choose also the factors f_i to be

$$\begin{cases} f_1(x, y) = (x + \zeta y)(x + \sigma^{3k}(\zeta)y), \\ f_2(x, y) = (x + \sigma^{2k}(\zeta)y)(x + \sigma^{5k}(\zeta)y), \\ f_3(x, y) = (x + \sigma^{4k}(\zeta)y)(x + \sigma^k(\zeta)y). \end{cases}$$

We have that $\phi_1 = f_1 f_2 f_3$ and as explained above these factors gives rise to the following linear system

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha(\zeta + \sigma^{3k}(\zeta)) + \beta(\sigma^{2k}(\zeta) + \sigma^{5k}(\zeta)) + \gamma(\sigma^{4k}(\zeta) + \sigma^k(\zeta)) = 0 \\ \alpha + \beta + \gamma = 0 \end{cases}$$

that obviously has infinite solutions. We pick the solution given by

$$\begin{cases} \alpha = -\sigma^{2k}(\zeta) - \sigma^{5k}(\zeta) + \sigma^{4k}(\zeta) + \sigma^k(\zeta) \\ \beta = \zeta + \sigma^{3k}(\zeta) - \sigma^{4k}(\zeta) - \sigma^k(\zeta) \\ \gamma = \sigma^{2k}(\zeta) + \sigma^{5k}(\zeta) - \zeta - \sigma^{3k}(\zeta) \end{cases}$$

As before, let $A(a, b) = \alpha f_1(a, b)$, $B(a, b) = \beta f_2(a, b)$, $C(a, b) = \gamma f_3(a, b)$ and since we have

$$A + B + C = 0$$

we can consider the Frey-curves

$$E_{(a,b)} : y^2 = x(x - A(a, b))(x + B(a, b)).$$

Proposition 2.8 *If $r = 6k + 1$ then the curves $E_{(a,b)}/K^+$ admit a model over K_0 .*

Proof: First observe that $\sigma^{2k} \pmod{\sigma^{3k}}$ has order 3 and generates $\text{Gal}(K^+/K_0)$. Since the curves E are defined over K^+ they are invariant under the order 2 element σ^{3k} and in particular $j(E)$ is invariant σ^{3k} . Moreover,

$$\sigma^{2k}(\alpha) = \beta, \quad \sigma^{2k}(\beta) = \gamma, \quad \sigma^{2k}(\gamma) = \alpha,$$

and also

$$\sigma^{2k}(f_1) = f_2, \quad \sigma^{2k}(f_2) = f_3, \quad \sigma^{2k}(f_3) = f_1,$$

then

$$\sigma^{2k}(A) = B, \quad \sigma^{2k}(B) = C, \quad \sigma^{2k}(C) = A.$$

Since

$$j(E) = 2^8 \frac{(AB + BC + CA)^3}{(ABC)^2}$$

it is clearly invariant under σ^{2k} then the j -invariant actually is in K_0 . Now we write $E_{(a,b)}$ in the short Weierstrass form to get a model

$$\begin{cases} E : y^2 = x^3 + a_4x + a_6, \text{ where} \\ a_4 = -432(AB + BC + CA) \\ a_6 = -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3) \end{cases}$$

Since a_4 is clearly invariant under σ^{2k} and

$$\begin{aligned} a_6 &= -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3) = \\ &= -1728(2(-B - C)^3 + 3(-B - C)^2B - 3(-B - C)B^2 - 2B^3) = \\ &= -1728(2B^3 + 3B^2C - 3BC^2 - 2C^3) = \sigma^{2k}(a_6) \end{aligned}$$

we conclude that the short Weierstrass model is already defined over K_0 . ■

Let π_2 and π_r denote a prime in K_0 above 2 and r , respectively.

Proposition 2.9 *The conductor of the curves $E_{(a,b)}$ over K_0 is of the form*

$$N_E = 2^s \pi_r^2 \text{rad}(c),$$

where s may be 2, 3 or 4.

Proof: Writing a curve in short Weierstrass form changes the values of Δ , c_4 and c_6 by a factor of 6^{12} , 6^4 and 6^6 . Since the primes dividing 6 do not ramify in K/K_0 and do not divide c the conductor of E at primes dividing c is the same as before.

Since $\pi_r = \mathfrak{P}_r^3$ in K^+ we see from the third paragraph in the proof of Proposition 2.4 that $v_{\pi_r}(\Delta(E)) = 4$ or 2 . Also, $v_{\pi_r}(c_4(E)) > 0$ and since we are in characteristic ≥ 5 this implies that the equation is minimal and has bad additive reduction with $v_{\pi_r}(N_E) = 2$.

It easily can be seen that $v_{\pi_2}(\Delta(E)) = 16$, $v_{\pi_2}(c_6(E)) = 11$ and $v_{\pi_2}(c_4(E)) \geq 8$. Table IV in [21] tell us that the equation is not minimal and after a change of variables we have $v_2(\Delta(E)) = 4$, $v_{\pi_2}(c_6(E)) = 5$ and $v_{\pi_2}(c_4(E)) \geq 4$. Now exactly as in the proof of Proposition 2.4 we can conclude that $v_{\pi_2}(N_E)$ may be 2, 3, or 4. ■

The existence of a model over K_0 has advantages. On one hand, Proposition 2.10 can be proved for the new model giving a smaller constant for $M(r)$; also, with modularity of the curves $E_{(a,b)}/K_0$ we can argue exactly as we did over K^+ to apply the results on level lowering. This would lead to the computation of Hilbert newforms over K_0 which is a number field of dimension k when *a priori* we were over K^+ of dimension $3k$. In a latter section we will use this fact to solve equations for $r = 7$ and in [9] the case $r = 13$ is treated in detail.

2.4 Modularity of E and Irreducibility of $\bar{\rho}_{E,p}$

Denote by $\rho_{E,3}$ and $\bar{\rho}_{E,p}$ the p -adic and the mod p representations associated with E . Two fundamental steps in the modular approach is to guarantee absolute irreducibility of $\bar{\rho}_{E,p}$ and modularity of the Frey-curves. We already know that these are requirements to apply the results on level lowering. For a fixed r , regarding irreducibility we have

Theorem 2.10 *There exists a constant $M(r)$ such that if $p > M(r)$ then the representation $\bar{\rho}_{E,p}$ is absolutely irreducible.*

Proof: Since $\bar{\rho}_{E,p}$ is odd and K^+ is totally real it is known that $\bar{\rho}_{E,p}$ is absolutely reducible if and only if it is reducible. Let p be a semistable prime for E and unramified in K^+ . Suppose that $\bar{\rho}_{E,p}$ is abs. reducible. Since it must be reducible over \mathbb{F}_p the fundamental characters of level 2 can not occur, hence $\bar{\rho}_{E,p}$ must have the form

$$\bar{\rho}_{E,p} = \begin{pmatrix} \epsilon^{-1}\chi_p & * \\ 0 & \epsilon \end{pmatrix}, \quad (9)$$

where χ_p is the mod p cyclotomic character and ϵ is a character of G_{K^+} with values in \mathbb{F}_p . Since the image of inertia at semistable primes is of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ the conductor of ϵ only contains bad additive primes. By the work of Carayol the conductor at bad additive primes of $\bar{\rho}_{E,p}$ is the same of $\rho_{E,p}$. Since the conductors of ϵ and ϵ^{-1} are equal it follows from proposition 2.4 that the $\text{cond}(\epsilon) = 2\mathfrak{P}_r$ or $2^2\mathfrak{P}_r$. The finite order characters of G_{K^+} with conductor dividing $2^2\mathfrak{P}_r$ are in correspondence with the characters of a finite group H whose order depends on r . In particular, if K^+ has narrow class number 1

they are in correspondence with the characters of $(\mathcal{O}_K/2^2\mathfrak{P}_r)^*$. The group of characters of H is dual of H then all the characters have order at most equal to the cardinality of H . In particular ϵ is a root of the polynomial $q_1 := x^{|H|} - 1 \pmod{p}$. Let \mathfrak{P}_3 be a prime above 3 and q the order of its residue field. Since E has good reduction at \mathfrak{P}_3 by taking traces on equality (9) we get

$$a_{\mathfrak{P}_3} \equiv \epsilon(\text{Frob}_{\mathfrak{P}_3}) + q\epsilon^{-1}(\text{Frob}_{\mathfrak{P}_3}) \pmod{p},$$

which implies that $\epsilon(\text{Frob}_{\mathfrak{P}_3})$ satisfies the polynomial $q_2 := x^2 - a_{\mathfrak{P}_3}x + q \pmod{p}$. Let $\zeta = \zeta_{|H|}$, then the resultant of q_1 and q_2 is given by

$$\begin{aligned} \text{res}(q_1, q_2) &= \prod_{i=1}^{|H|} \left(\frac{a_{\mathfrak{P}_3} + \sqrt{a_{\mathfrak{P}_3}^2 - 4q}}{2} - \zeta^i \right) \left(\frac{a_{\mathfrak{P}_3} - \sqrt{a_{\mathfrak{P}_3}^2 - 4q}}{2} - \zeta^i \right) \\ &= \prod_{i=1}^{|H|} (\zeta^{2i} - a_{\mathfrak{P}_3}\zeta^i + q) \end{aligned}$$

Since $a_{\mathfrak{P}_3}$ is an integer such that $|a_{\mathfrak{P}_3}| \leq \sqrt{q}$ we have

$$|\text{res}(q_1, q_2)| \leq \prod_{i=1}^{|H|} (|\zeta|^{2i} + |a_{\mathfrak{P}_3}||\zeta|^i + q) \leq \prod_{i=1}^{|H|} (1 + \sqrt{q} \times 1 + q) \leq (1 + \sqrt{q} + q)^{|H|}$$

Moreover, $\epsilon(\text{Frob}_{\mathfrak{P}_3})$ is a common root of the $q_i \pmod{p}$ then $\text{res}(q_1, q_2) \equiv 0 \pmod{p}$ which is impossible if $p > (1 + \sqrt{q} + q)^{|H|}$. Thus the theorem hold if we take $M(r) = (1 + \sqrt{q} + q)^{|H|}$. \blacksquare

The proof of the previous theorem is quite general. Indeed, a closer look shows that it only depends on K^+ being totally real and on the existence of a concrete prime with good reduction for $E_{(a,b)}$. Actually, using more information about our curves we can prove a much better result in some cases. Recall that K^+/\mathbb{Q} is Galois then inertial degree $f = f(\mathfrak{P}_2/2)$ is the same for all primes \mathfrak{P}_2 above 2.

Theorem 2.11 *If the inertial degree f is odd then $\bar{\rho}_{E,p}$ is irreducible for all primes $p \geq 3$.*

Proof: Let \mathfrak{P}_2 be a prime above 2 and since E has potentially good reduction at \mathfrak{P}_2 let $\Phi_{\mathfrak{P}_2}$ be defined as in [17]. Since $v_{\mathfrak{P}_2}(\Delta) = 4 \not\equiv 0 \pmod{3}$ we are in case (ii) of Theorem 3 in [17]. It follows from the last paragraph of the proof of Proposition 2.4 that $E_{(a,b)}$ may have Kodaira types II, III and IV at \mathfrak{P}_2 . Then from Theorem 3 in [17] follows that $|\Phi_{\mathfrak{P}_2}| = 3$ or 24. Since $2^{nf}(2^f - 1)$ is divisible by 3 only if f is even it follows from Proposition 3.3 in [1] that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 3$ if f is odd. \blacksquare

It is know that all elliptic curves over \mathbb{Q} are modular and is expected the same to be true over totally real number fields but there are no complete general results in the latter situation. Thus, in general, we do not have modularity of our Frey-curves $E_{(a,b)}$.

Conjecture 2.12 *The curves $E_{(a,b)}$ over K^+ or K_0 are modular.*

The conjecture above is true in some cases. If $r = 7$ then the Frey-curve is defined over \mathbb{Q} (see section 3.1) hence it is modular. Also, Theorem 4.1 in [9] states that an elliptic curve C over a totally real cyclic field F with good reduction at the primes above 3 is modular if 3 splits in F . As a corollary the conjecture holds for $r = 13$.

We will now make a few comments on the general case. In [9] the proof of modularity is divided into 3 cases: (i) $\bar{\rho}_{E,3}$ and $\bar{\rho}_{E,3}|G_{F(\sqrt{-3})}$ both abs. irreducible; (ii) $\bar{\rho}_{E,3}$ abs. irreducible and $\bar{\rho}_{E,3}|G_{F(\sqrt{-3})}$ reducible; (iii) $\bar{\rho}_{E,3}$ reducible. When trying to mimic the proof for the general case we will have trouble due to the fact that 3 is not necessarily split in K^+ , because in that case we can not guarantee the existence of an ordinary lifting of $\bar{\rho}_{E,3}$ (in the residually ordinary case) by means of Breuil's results. In section 6 of [11] the authors prove modularity lifting without assuming ordinarity at specific places. Unfortunately, the results there are limited for the case $p = 3$. In a mail conversation with T. Gee we have learned that the generalization of the theorems there to $p = 3$ (possibly with some additional restrictions on the image of the mod p Galois representation) should follow from current techniques. In this scenario we can expect the curves $E_{(a,b)}$ to be proven modular in case (i), where we apply this more general result instead of Corollary 2.1.3 in [16]. And if the curve has ordinary good reduction at all primes above 3 also in case (iii), where modularity follows from an application of Theorem A in [26]. With these observations in mind we may be able to achieve modularity for particular values of r : we first check if $\bar{\rho}_{E,3}$ is abs. irreducible, for example via Proposition 2.11), to conclude that we are in case (i) or (ii); secondly by computing the 3-division polynomial and verifying that it is irreducible over $K^+(\sqrt{-3})$ (or $K_0(\sqrt{-3})$) we conclude that we are in case (i). On the other hand, if we can only exclude case (ii) modularity also follows if we have that the Frey-curves are ordinary at all primes above 3. This can be seen by computing all the possible values $a_{\mathfrak{p}_3}(E_{(a,b)})$ for all $(a,b) \neq (0,0)$ in \mathbb{F}^2 where \mathbb{F} is the residual field at \mathfrak{p}_3 and checking that $3 \mid a_{\mathfrak{p}_3}$ never happens.

3 Application: the case $r = 7$

In this section we will use the strategy described before to study the equation of signature $(7, 7, p)$. Then we will also see that the same Frey-curve can be used to attack equations of the form $\phi(x, y) = dz^p$, where ϕ is a degree six homogeneous form and actually prove a theorem for $d = 71$.

3.1 The equation $x^7 + y^7 = Cz^p$

We will prove the following theorem

Theorem 3.1 *Let $d = 2^{s_0}3^{s_1}5^{s_2}$ and γ be an integer only divisible by primes $l \not\equiv 1 \pmod{7}$. Then, if $p \geq 17$ we have that*

- (I) *The equation $x^7 + y^7 = d\gamma z^p$ has no non-trivial first case solutions if (s_0, s_1, s_2) satisfies any of the following three conditions $(\geq 2, \geq 0, \geq 0)$, $(= 1, \geq 1, \geq 0)$ or $(= 0, \geq 0, \geq 1)$.*

(II) The equation $x^{14} + y^{14} = d\gamma z^p$ has no non-trivial primitive solutions if $s_2 > 0$ or $s_3 > 0$ or $s_0 \geq 2$.

We will start by proving (I) by following the strategy delineated in the previous section. Observe that $7 = 6k + 1$ for $k = 1$, that is, we are in a case of less computational requirements and $K_0 = \mathbb{Q}$. Since γ will never be used in the proof we suppose that $\gamma = 1$. Let (a, b, c) be a non-trivial primitive solution to the equation

$$x^7 + y^7 = (x + y)\phi_7(x, y) = dz^p. \quad (10)$$

With the notation of the previous section we have $(\phi_7 =)\phi = \phi_1$ and there must exist a non-trivial primitive solution (a, b, c) to

$$\phi(a, b) = c^p, \quad (11)$$

with $d \mid a + b$ and $7 \nmid a + b$ or to

$$\phi(a, b) = 7c^p \quad (12)$$

with $d \mid a + b$ and $7 \mid a + b$, where in both cases c is only divisible by primes congruent to 1 modulo 7.

We now construct the F-H-curves attached to the solution (a, b, c) . Let $\zeta = \zeta_7$ be a 7-root of unity, by following the construction in the previous section we get $\phi = f_1 f_2 f_3$, with

$$\begin{aligned} f_1(x, y) &= x^2 + (\zeta + \zeta^6)xy + y^2 \\ f_2(x, y) &= x^2 + (\zeta^4 + \zeta^3)xy + y^2 \\ f_3(x, y) &= x^2 + (\zeta^5 + \zeta^2)xy + y^2 \end{aligned}.$$

and we find a triple (α, β, γ) given by

$$\begin{cases} \alpha = \zeta^5 - \zeta^4 - \zeta^3 + \zeta^2 \\ \beta = -2\zeta^5 - \zeta^4 - \zeta^3 - 2\zeta^2 - 1 \\ \gamma = \zeta^5 + 2\zeta^4 + 2\zeta^3 + \zeta^2 + 1. \end{cases}.$$

This results in the F-H-curves with short Weierstrass form defined over \mathbb{Q} and model $E_{(a,b)} : y^2 = x^3 + a_4x + a_6$, where

$$\begin{cases} a_4 = -3024(a^4 - a^3b + 3a^2b^2 - ab^3 + b^4) \\ a_6 = 12096(a^6 - 15a^5b + 15a^4b^2 - 29a^3b^3 + 15a^2b^4 - 15ab^5 + b^6). \end{cases}$$

These curves were already known to Kraus (in [20] he gives a Frey-curve with the same short Weierstrass model of ours) and Dahmen also found a twist of them with a different method in [7]. Since $\alpha\beta\gamma = -7$ the discriminant is of the form

$$\Delta(E) = 2^{16}3^{12}7^{2+s}c^2, \quad (13)$$

where $s = 0$ or $s = 2$ if (a, b, c) is a solution to (11) or (12), respectively.

Proposition 3.2 *If $(a, b) = 1$ the curves $E_{(a,b)}$ have conductor given by*

$$N_E = \begin{cases} 2^2 7^2 \text{rad}(c) \text{ or } 2^3 7^2 \text{rad}(c) & \text{if } 2 \nmid a + b \\ 2^4 7^2 \text{rad}(c) & \text{if } 2 \parallel a + b \\ 2^3 7^2 \text{rad}(c) & \text{if } 4 \mid a + b \end{cases}$$

Moreover, if $2 \nmid a+b$ we can suppose that a is even and the conductor is

$$N_E = \begin{cases} 2^2 7^2 \text{rad}(c) & \text{if } 4 \mid a \\ 2^3 7^2 \text{rad}(c) & \text{if } 4 \nmid a \end{cases}$$

Proof: From Proposition 2.9 we know the set of possible values for the conductor. With the help of SAGE we compute the values of the conductor for all pairs $(a, b) \bmod 2^6$ and observe how they relate to $a+b$. ■

By the Frey-Hellegouarch argument we conclude that $\bar{\rho}_{E,p}$ does not ramify at primes dividing c . Let $S_2(M)$ denote the set of cusp forms of weight 2, trivial nebentypus and level M . Since (a, b, c) is non-trivial there exists a semistable prime greater than 6 then from the work of Mazur (see ?) if $p \geq 17$ we have that $\bar{\rho}_{E,p}$ is absolutely irreducible (see also Theorem 22 in [7]). By Serre's strong conjecture (now a theorem due to Khare-Wintenberger, see [14] and [15]) there must exist a newform $f \in S_2(N_0)$ where $N_0 = 2^s 7^2$ with $s = 2, 3$ or 4 such that

$$\rho_{E,p} \equiv \rho_{f,p} \bmod \mathfrak{P}, \quad (14)$$

for some prime \mathfrak{P} in $\bar{\mathbb{Q}}$ above p . To finish the argument we need to contradict (14). Using SAGE software we compute the newforms in $S_2(N_0)$ for the values of N_0 determined above and divide them into two sets

- S1: Newforms with $\mathbb{Q}_f = \mathbb{Q}$
- S2: Newforms such that \mathbb{Q} is strictly contained in \mathbb{Q}_f

Now we will look for a contradiction to (14) for each newform in both sets, starting with S1. For each pair $(a, b) \bmod l$ with $l \in \{3, 5, 11, 13, 17, 19, 23\}$ we computed with SAGE all the possible values a_l for our Frey-curves $E_{(a,b)}$:

$$\begin{cases} a_3 \in \{-1, 3\}, \\ a_5 \in \{-3, -1, 1, 3\}, \\ a_{11} \in \{-5, -3, 1, 3\}, \\ a_{13} \in \{-6, -2, 2, 6\}, \\ a_{17} \in \{-5, -3, 1, 3, 5\}, \\ a_{19} \in \{-7, -5, 1, 5, 7\}, \\ a_{23} \in \{-9, -7, -5, -1, 1, 3\} \end{cases}$$

Furthermore, we also see that

$$a_l(E_{(a,b)}) = -1 \quad \text{if} \quad l = 3 \text{ or } 5 \quad \text{and} \quad l \mid a+b. \quad (15)$$

As long as $p > 7$ by comparing the coefficients of the forms in S1 against the previous values we find a contradiction to congruence (14) for all f in S1 except for the newforms corresponding to the curves $E_{(0,1)}$, $E_{(1,-1)}$ and $E_{(1,1)}$. These three forms were expected to survive since $(0, 1, 1)$ and $(1, 1, 1)$ are solutions of (11) and $(1, -1, 1)$ is a solution of (12). Since these curves have no complex multiplication in order to eliminate them we need to use the information $d \mid a+b$. By Proposition 3.2 we see that if (s_0, s_1, s_2) satisfies the conditions $(\geq 0, \geq 0, \geq$

1), $(= 1, \geq 1, \geq 0)$ or $(\geq 2, \geq 0, \geq 0)$ to finish the proof we have to eliminate $(E_{(0,1)}, E_{(1,-1)}, E_{(1,1)})$, $(E_{(1,-1)}, E_{(1,1)})$ or $E_{(1,-1)}$, respectively. Observing that

$$(a_3(E_{(0,1)}), a_3(E_{(1,-1)}), a_3(E_{(1,1)})) = (-1, -1, 3)$$

and

$$(a_5(E_{(0,1)}), a_5(E_{(1,-1)}), a_5(E_{(1,1)})) = (-3, -1, 1)$$

we see that the conditions in (s_0, s_1, s_2) together with (15) are enough to deal with $E_{(0,1)}$ and $E_{(1,1)}$ but not with $E_{(1,-1)}$ as expected.

To eliminate $E_{(1,-1)}$ we will use the inertia at 7. Let C/\mathbb{Q} be an elliptic curve and $\Phi_7(C)$ be the Galois group of the extension of \mathbb{Q} where C acquire good reduction at 7. By following Kraus (see [17]) we know that

$$|\Phi_7(C)| = \text{denominator of } \left(\frac{\nu_7(\Delta_{\min}(C))}{12} \right),$$

and by formula (13) we find that $|\Phi_7(E_{(a,b)})| = 3$ or 6 , if $7 \mid a+b$ or $7 \nmid a+b$, respectively. In particular $|\Phi_7(E_{(1,-1)})| = 3$ and (14) can not hold if $7 \nmid a+b$, because the inertia at 7 do not match. This eliminates all the newforms in S1 if our putative solution (a, b, c) is a first case solution (see Definition 1.1).

Now suppose that (14) holds for some f in S2 then the congruence

$$a_3(E) \equiv c_3(f) \pmod{\mathfrak{P}} \quad (16)$$

must hold, for some newform $f = q + \sum_{n=2} c_n q^n$ in S2 and a prime \mathfrak{P} in $\bar{\mathbb{Q}}$ above p . This is not possible if $p > 7$. Indeed, for all newforms in S2 the minimal polynomial of the Fourier coefficient c_3 is $x^2 - 2$ or $x^2 - 8$ then, for example, in the latter case we must have

$$0 \equiv c_3^2 - 8 \equiv a_3^2 - 8 \pmod{p}.$$

Since our curves verify $a_3 \in \{-1, 3\}$ the previous congruence implies that $0 \equiv -7, 1 \pmod{\mathfrak{P}}$ which is impossible if $p > 7$. The same holds with the other minimal polynomial and this concludes the proof of part (I) of Theorem 3.1. ■

We will now prove part (II). By looking modulo 3 and 4 we find that $a^2 + b^2$ with $(a, b) = 1$ is never divisible by 3 and 4. Then, from the factorization

$$a^{14} + b^{14} = (a^2 + b^2)\phi(a^2, b^2) = dc^p$$

and the fact that $d \mid a^2 + b^2$ it is clear that if $s_0 \geq 2$ or $s_1 > 0$ the theorem holds. We are left to deal with the case of $d = 5^{s_3}$. Again, by looking modulo 7 we find that $a^2 + b^2$ is never divisible by 7 then we can translate $a^{14} + b^{14} = (a^2 + b^2)\phi(a^2, b^2) = dc^p$ into the equation

$$\phi(a^2, b^2) = c_0^p,$$

with $d \mid a^2 + b^2$. Given a primitive solution (a, b, c) we use $E = E_{(a^2, b^2)}$ has a Frey-curve. From the observation modulo 4, Proposition 3.2 and Serre's strong conjecture it follows that the possible levels for newforms satisfying congruence

$$\rho_{E,p} \equiv \rho_{f,p} \pmod{\mathfrak{P}}$$

are $2^2 7^2$ or $2^4 7^2$. We do as above and divide the newforms into the same sets S1 and S2. This time the newform associated with the solution $(1, -1, 0)$ is not a possible choice in S1 hence the restriction $7 \nmid c$ is not needed. Since $d \mid a^2 + b^2$ we have $a_5(E_{(a^2, b^2)}) = -1$ and as we already know this is enough to deal with $E_{(0,1)}$ and $E_{(1,1)}$ eliminating all the newforms in S1. The newforms in S2 are eliminated exactly as in the proof of (I). \blacksquare

3.2 The equation $\phi(x, y) = 71z^p$

From the discriminant of the curves $E_{(a,b)}$ it is clear that we can use them to attack equations of the form $\phi(x, y) = dz^p$, where

$$\phi(x, y) = x^6 - x^5y + x^4y^2 - x^3y^3 + x^2y^4 - xy^5 + y^6$$

is the same polynomial of the previous section. Recall that if $(a, b) = 1$ then $\phi(a, b)$ is only divisible by primes congruent to 1 modulo 7. We will now prove the following result

Theorem 3.3 *If $p > 254^{2873}$ is a prime, then the equation*

$$\phi(x, y) = 71z^p \tag{17}$$

has no non-trivial primitive solution (a, b, c) such that $71 \nmid c$.

Suppose that (a, b, c) is a non-trivial primitive solution of (17) and consider the same Frey-curves $E_{(a,b)}$ as before. The discriminant of E is of the form

$$\Delta(E) = 2^{16} 3^{12} 7^s 71^2 c^{2p}.$$

Denote by c_0 the product of the primes $q \neq 71$ dividing c .

Proposition 3.4 *The curves $E_{(a,b)}$ have conductor given by*

$$N_E = 2^s 7^2 71 c_0,$$

where $s \in \{2, 3, 4\}$.

Proof: The same proof of Proposition 3.2 works for all primes $p \neq 71$. For $p = 71$ observe that $v_p(\Delta) \geq 2$ for all (a, b) . Since 71 splits in K_0 , A, B, C are conjugates and coprimes at 71 we know that each of them has one prime factor (in K_0) of 71. Since

$$c_4 = 2^4(AB + BC + AC)$$

it is clear that $v_p(c_4) = 0$. Then $E_{(a,b)}$ has multiplicative reduction at $p = 71$. \blacksquare

Since all the primes q dividing c_0 are of semistable reduction we can apply the Frey-Hellgouarch argument to conclude that $\bar{\rho}_{E,p}$ will not ramify at $q \mid c_0$. As in the previous section we have that $\bar{\rho}_{E,p}$ is absolutely irreducible for $p \geq 17$ then again by Serre's strong conjecture there must exist a newform f in $S_2(N_0)$ where $N_0 = 2^s 7^2 71$ with $s \in \{2, 3, 4\}$ such that

$$\rho_{E,p} \equiv \rho_{f,p} \pmod{\mathfrak{P}}. \tag{18}$$

The space $S_2^{new}(2^4 7^2 71)$ is too large to be computable with SAGE. Nevertheless, we are able to finish the proof but the price of doing it without computing that space is the large bound for p in the statement of Theorem 3.3. As before divide the newforms in the spaces $S_2(N_0)$ where $N_0 = 2^s 7^2 71$ with $s \in \{2, 3, 4\}$ into two sets:

S1: Newforms with $\mathbb{Q}_f = \mathbb{Q}$

S2: Newforms such that \mathbb{Q} is strictly contained in \mathbb{Q}_f

Since the newforms in S1 correspond to elliptic curves over \mathbb{Q} we use SAGE to consult Cremona's Table of elliptic curves for conductors up to 130000 to get the complete list of elliptic curves with conductor $2^s 7^2 71$ for $s = 2, 3, 4$. For each curve in the list we computed the values a_q for $q \in \{3, 5, 11, 13, 17, 19, 23\}$. Comparing these a_q with the few possibilities allowed to our Frey-curves listed in the previous section we can eliminate all the curves.

To deal with the newforms $f = q + \sum_{n=2} c_n q^n$ in S2 we will use the Weil bound $|c_l| \leq 2\sqrt{l}$ and the following proposition.

Proposition 3.5 *If f is a newform such that $\mathbb{Q}_f \neq \mathbb{Q}$ then there exists a prime number $q \leq SB$ such that the coefficient $c_q(f)$ does not belong to \mathbb{Q} , where SB (Sturm bound) is given by*

$$SB = \frac{N_0}{6} \prod_{\text{primes } q|N_0} \left(1 + \frac{1}{q}\right)$$

Proof: See [18], Lemme 1.

Now suppose that (18) holds for an f in S2 and let q be a prime given by the proposition above. We can suppose that f is of level $2^4 7^2 71$ because the smaller levels would give smaller bounds for p . We use SAGE to compute the dimension D of the space $\mathcal{S}_2^{new}(2^4 7^2 71)$, which gives $D = 1435$ and the Sturm bound $SB = 16128$. Then we have

$$\begin{cases} |a_q|, |c_q| \leq 2\sqrt{q} \leq 2\sqrt{SB} \leq 254 \\ [\mathbb{Q}_f : \mathbb{Q}] \leq D = 1435 \end{cases}$$

and also

$$a_q(E) \equiv c_q \pmod{\mathfrak{P}}.$$

Let $p_c(x)$ be the minimal polynomial of c_q , which is of degree at most D , and can not have integer roots because c_q is not an integer. Then $p_c(a_q) \neq 0$ and

$$p_c(a_q) \equiv p_c(c_q) \equiv 0 \pmod{\mathfrak{P}}.$$

Since there are only a finite number of possibilities for a_q then also for $p_c(a_q(E))$ thus there is a constant C such that if $p > C$, the congruence $p_c(a_q(E)) \equiv 0 \pmod{p}$ can not hold.

Now we proceed to the computation of a concrete value for C . First observe that the roots r_i of p_c are the Galois conjugates c_q^σ of c_q and they also satisfy $|r_i| \leq 2\sqrt{q} \leq 254$. Let b_n be the coefficients of $p_c = \sum b_n x^n$. Since we know that the b_n are given by the symmetric functions in r_i we can find an upper bound for each b_n easily, for example

$$b_{n-2} = r_0 r_1 + r_0 r_2 + \dots + r_{n-2} r_{n-1} \leq \binom{1435}{2} 254^2,$$

and the biggest upper bound that we find this way is $\binom{1435}{1430} 254^{1430}$. Hence we have

$$|p_c(x)| \leq 1435(\max\{b_n\})|x|^{1435}$$

and thus

$$|p_c(a_q(E))| \leq 1435 \binom{1435}{1429} 254^{1429} 254^{1435} \leq 254^2 254^7 254^{2864} \leq 254^{2873},$$

where the last two inequalities were taken only for aesthetic purposes. Then taking $C = 254^{2873}$ ends the proof of Theorem 3.3. \blacksquare

4 Examples: the cases $r = 11, 13, 17, 19$

4.1 The equation $x^{11} + y^{11} = Cz^p$

Note that $11 \equiv -1 \pmod{6}$ so this is computationally difficult case. Following the method we pick $\phi_1 = f_1 f_2 f_3$, where

$$\begin{cases} f_1(x, y) = x^2 + (\zeta + \zeta^{10})xy + y^2, \\ f_2(x, y) = x^2 + (\zeta^2 + \zeta^9)xy + y^2, \\ f_3(x, y) = x^2 + (\zeta^3 + \zeta^8)xy + y^2. \end{cases}$$

Let (a, b, c) be a non-trivial primitive solution of

$$x^{11} + y^{11} = Cz^p, \quad (19)$$

then for some unit $\mu \in K^+$ we also have a non-trivial primitive solution of

$$\phi_1(x, y) = \mu z^p \quad (20)$$

or

$$\phi_1(x, y) = \mu \pi_{11}^3 z^p \quad (21)$$

if $11 \nmid a+b$ or $11 \mid a+b$, respectively. The resulting F-H-curves over K^+ is given by

$$E_{(a,b)} : y^2 = x^3 + a_4 x + a_6, \text{ where}$$

$$\begin{aligned} a_4(a, b) &= (432w^3 - 432w - 2592)a^4 \\ &\quad + (-432w^4 - 3888w^3 + 1296w^2 + 7776w + 3024)a^3b \\ &\quad + (3456w^3 - 432w^2 - 6480w - 8208)a^2b^2, \\ &\quad + (-432w^4 - 3888w^3 + 1296w^2 + 7776w + 3024)ab^3 \\ &\quad + (432w^3 - 432w - 2592)b^4 \\ a_6(a, b) &= (8640w^4 + 25920w^3 - 39744w^2 - 48384w + 5184)a^6 \\ &\quad + (5184w^4 - 98496w^3 + 10368w^2 + 176256w + 139968)a^5b \\ &\quad + (285120w^3 - 57024w^2 - 570240w - 171072)a^4b^2 \\ &\quad + (25920w^4 - 302400w^3 - 5184w^2 + 596160w + 338688)a^3b^3 \\ &\quad + (285120w^3 - 57024w^2 - 570240w - 171072)a^2b^4 \\ &\quad + (5184w^4 - 98496w^3 + 10368w^2 + 176256w + 139968)ab^5 \\ &\quad + (8640w^4 + 25920w^3 - 39744w^2 - 48384w + 5184)b^6 \end{aligned}$$

where the minimal polynomial of w is $t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1$. We observe that 3 is inert in K^+ and with the help of SAGE we computed $a_3(E_{(a,b)})$ for all pairs $(a, b) \pmod{3}$ and obtained that $a_3(E) \in \{-16, 16\}$ which shows that $E_{(a,b)}$ are ordinary at 3.

4.2 The equation $x^{13} + y^{13} = Cz^p$

Note that $13 \equiv 1 \pmod{6}$ so this is a good case. This equation is studied in detail in joint work with L. Dieulefait (see [9]). The Frey-curves used there can be obtained as a particular case of our recipe with $K_0 = \mathbb{Q}(w)$, where $w^2 = 13$ and the curves are given by

$$E_{(a,b)} : y^2 = x^3 + a_4(a, b)x + a_6(a, b), \text{ where}$$

$$\begin{aligned} a_4(a, b) &= (216w - 2808)a^4 + (-1728w + 5616)a^3b \\ &\quad + (1728w - 11232)a^2b^2 + (-1728w + 5616)ab^3 \\ &\quad + (216w - 2808)b^4, \\ a_6(a, b) &= (-8640w + 44928)a^6 + (49248w - 235872)a^5b \\ &\quad + (-129600w + 471744)a^4b^2 + (152928w - 662688)a^3b^3 + \\ &\quad + (-129600w + 471744)a^2b^4 + (49248w - 235872)ab^5 + \\ &\quad + (-8640w + 44928)b^6 + (50193w + 182520)b^6. \end{aligned}$$

Although we are in good computational case the dimension of $S_2(2^4w^2)$ is already too big for completely compute the whole subspace of newforms. In order to solve this difficulty an algorithm of John Voight was used to compute only the newforms with field of coefficients equal to \mathbb{Q} . Moreover, modularity of the curves are proved and we achieve the following result (see [9]).

Theorem 4.1 *Let $d = 3, 5, 7$ or 11 and γ be an integer divisible only by primes $l \not\equiv 1 \pmod{13}$. If $p > 4992539$ is a prime, then:*

- (I) *The equation $x^{13} + y^{13} = d\gamma z^p$ has no non-trivial primitive first case solutions.*
- (II) *The equation $x^{26} + y^{26} = 2d\gamma z^p$ has no primitive non-trivial solutions.*

4.3 The equation $x^{17} + y^{17} = Cz^p$

Note that $17 \equiv -1 \pmod{6}$ so this is a bad case. Following the method we pick $\phi_1 = f_1 f_2 f_3$, with

$$\begin{cases} f_1(x, y) = x^2 + (\zeta + \zeta^{16})xy + y^2, \\ f_2(x, y) = x^2 + (\zeta^2 + \zeta^{15})xy + y^2, \\ f_3(x, y) = x^2 + (\zeta^3 + \zeta^{14})xy + y^2. \end{cases}$$

Let (a, b, c) be a non-trivial primitive solution of

$$x^{17} + y^{17} = Cz^p, \tag{22}$$

then for some unit $\mu \in K^+$ we also have a non-trivial primitive solution of

$$\phi_1(x, y) = \mu z^p \quad (23)$$

or

$$\phi_1(x, y) = \mu \pi_{17}^3 z^p \quad (24)$$

if $17 \nmid a + b$ or $17 \mid a + b$, respectively. The resulting F-H-curves over K^+ are given by

$$E_{(a,b)} : y^2 = x^3 + a_4x + a_6, \text{ where}$$

$$\begin{aligned} a_4(a, b) = & (-432w^6 + 432w^5 + 2592w^4 - 1728w^3 - 3888w^2 + 1728w - 1728)a^4 \\ & + (-432w^7 + 3024w^6 + 2160w^5 - 15984w^4 - 3456w^3 + 19872w^2 \\ & + 1728w + 432)a^3b + (-3024w^6 + 1728w^5 + 16416w^4 - 6048w^3 \\ & - 22032w^2 + 4320w - 3888)a^2b^2 + (-432w^7 + 3024w^6 + 2160w^5 \\ & - 15984w^4 - 3456w^3 + 19872w^2 + 1728w + 432)ab^3 + (-432w^6 \\ & + 432w^5 + 2592w^4 - 1728w^3 - 3888w^2 + 1728w - 1728)b^4 \end{aligned}$$

$$\begin{aligned} a_6(a, b) = & (-8640w^7 + 25920w^6 + 46656w^5 - 143424w^4 - 62208w^3 + 196992w^2 \\ & + 3456w - 19008)a^6 + (5184w^7 - 93312w^6 + 25920w^5 + 497664w^4 \\ & - 160704w^3 - 663552w^2 + 150336w - 20736)a^5b + (-51840w^7 \\ & + 254016w^6 + 238464w^5 - 1316736w^4 - 295488w^3 + 1653696w^2 \\ & + 82944w - 72576)a^4b^2 + (39744w^7 - 269568w^6 - 101952w^5 \\ & + 1397952w^4 - 53568w^3 - 1802304w^2 + 114048w)a^3b^3 \\ & + (-51840w^7 + 254016w^6 + 238464w^5 - 1316736w^4 - 295488w^3 \\ & + 1653696w^2 + 82944w - 72576)a^2b^4 + (5184w^7 - 93312w^6 \\ & + 25920w^5 + 497664w^4 - 160704w^3 - 663552w^2 + 150336w \\ & - 20736)ab^5 + (-8640w^7 + 25920w^6 + 46656w^5 - 143424w^4 \\ & - 62208w^3 + 196992w^2 + 3456w - 19008)b^6 \end{aligned}$$

where the minimal polynomial of w is $t^8 + t^7 - 7t^6 - 6t^5 + 15t^4 + 10t^3 - 10t^2 - 4t + 1$. We observe that 3 is inert in K^+ and with the help of SAGE we computed $a_3(E_{(a,b)})$ for all pairs $(a, b) \pmod{3}$ and obtained that $a_3(E) \in \{-94, -62, 118\}$ which shows that $E_{(a,b)}$ are ordinary at 3.

4.4 The equation $x^{19} + y^{19} = Cz^p$

Note that $19 \equiv 1 \pmod{6}$ so this is a good case. Following the method we pick $\phi_1 = f_1 f_2 f_3$, with

$$\begin{cases} f_1(x, y) = x^2 + (\zeta + \zeta^{18})xy + y^2, \\ f_2(x, y) = x^2 + (\zeta^{12} + \zeta^7)xy + y^2, \\ f_3(x, y) = x^2 + (\zeta^{11} + \zeta^8)xy + y^2. \end{cases}$$

Let (a, b, c) be a non-trivial primitive solution of

$$x^{19} + y^{19} = Cz^p. \quad (25)$$

Then for some unit $\mu \in K_0$ we also have a non-trivial primitive solution of

$$\phi_1(x, y) = \mu z^p \quad (26)$$

or

$$\phi_1(x, y) = \mu \pi_{19}^3 z^p \quad (27)$$

if $19 \nmid a + b$ or $19 \mid a + b$, respectively. The resulting F-H-curves over K_0 are given by

$$E_{(a,b)} : y^2 = x^3 + a_4 x + a_6, \text{ where}$$

$$\begin{aligned} a_4(a, b) &= (864w^2 - 6480)a^4 \\ &\quad + (-3456w^2 - 432w + 20304)a^3b \\ &\quad + (4320w^2 - 432w - 29808)a^2b^2 \\ &\quad + (-3456w^2 - 432w + 20304)ab^3 \\ &\quad + (864w^2 - 6480)b^4, \\ a_6(a, b) &= (-34560w^2 + 5184w + 195264)a^6 \\ &\quad + (150336w^2 - 25920w - 922752)a^5b \\ &\quad + (-342144w^2 + 31104w + 1985472)a^4b^2 \\ &\quad + (418176w^2 - 76032w - 2548800)a^3b^3 \\ &\quad + (-342144w^2 + 31104w + 1985472)a^2b^4 \\ &\quad + (150336w^2 - 25920w - 922752)ab^5 \\ &\quad + (-34560w^2 + 5184w + 195264)b^6, \end{aligned}$$

where the minimal polynomial of w is $t^3 + t^2 - 6t - 7$. Here 3 is also inert in K^+ and computations allowed to see that $a_3(E) \in \{-1, 7\}$ which shows that the curves $E_{(a,b)}$ are ordinary at 3.

Although we are in a case of favorable computer requirements the dimension of $S(\mathfrak{P}_2^4 \mathfrak{P}_{19}^2)$ is 437761 which is already too big even for computing with John Voight algorithm only the newforms with coefficients in \mathbb{Q} as it was done in [9].

5 The case $r = 4m + 1$

In this section we will construct two extra Frey-curves attached to solutions of the equation $x^r + y^r = Cz^p$ for primes with form $r = 4m + 1$. The ideas here generalize the method in [10]. We first need to introduce the following definition analogously to that of \mathbb{Q} -curve.

Definition 5.1 *Let k be a number field and $G_k = \text{Gal}(\bar{\mathbb{Q}}/k)$ its absolute Galois group. We will say that an elliptic curve C is a k -curve if for every $\sigma \in G_k$ there exists an isogeny $\phi_\sigma : {}^\sigma C \rightarrow C$ defined over $\bar{\mathbb{Q}}$*

Let $\zeta := \zeta_r$ and $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ be the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta)$. Since $r = 4m + 1$ then K^+ has degree $2m$ and there exists a subfield $k \subset K^+$ such that $[K^+/k] = 2$ and $[k/\mathbb{Q}] = m$. Now we are going to construct Frey-curves over K^+ and show that they are k -curves. This way their attached Galois representations can be extended to k .

Let σ be the generator of $\text{Gal}(K^+/\mathbb{Q})$ then σ^m generates $\text{Gal}(K^+/k)$. Recall that $x^r + y^r = (x+y)\phi_r(x, y)$ and that $\phi_r(x, y)$ factors as a product of $2m$ degree two polynomials f_i with coefficients in K^+ . In particular, if (a, b, c) is a non-trivial primitive solution of $x^r + y^r = Cz^p$ the same argument as in section 1 tells us that for some unit $\mu \in K^+$ there must exist a non-trivial primitive solution (a, b, c_1) such that $C \mid a + b$ to

$$\phi_1(x, y) = \mu z^p \quad \text{or} \quad \phi_1(x, y) = \mu \pi_r^2 z^p, \quad (28)$$

if $r \nmid a + b$ or $r \mid a + b$, respectively, and $\phi_1 = f_1 f_2$ where

$$\begin{cases} f_1(x, y) = x^2 + (\zeta + \zeta^{4m})xy + y^2 \\ f_2(x, y) = x^2 + \sigma^m(\zeta + \zeta^{4m})xy + y^2. \end{cases}$$

In order to construct an useful k -curve we first need to find α, β such that $(a + b)^2 = \alpha f_1(a, b) + \beta f_2(a, b)$. That is, solve the linear system

$$\begin{cases} \alpha + \beta = 1 \\ \alpha(\zeta + \zeta^{4m}) + \beta\sigma^m(\zeta + \zeta^{4m}) = 2, \end{cases}$$

which has a solution for $\alpha, \beta \in K^+$ given by

$$\begin{cases} \alpha = (\sigma^m(\zeta + \zeta^{4m}) - 2)(\sigma^m(\zeta + \zeta^{4m}) - \zeta^m - \zeta)^{-1} \\ \beta = (2 - (\zeta + \zeta^{4m}))(\sigma^m(\zeta + \zeta^{4m}) - \zeta - \zeta^{4m})^{-1}, \end{cases}$$

that easily can be seen to satisfy $\sigma^m(\alpha) = \beta$. Now we can consider the Frey-curves

$$E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 + \alpha f_1(a, b)x,$$

having Galois conjugate by σ^m

$$\sigma^m E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 + \beta f_2(a, b)x,$$

with the 2-isogeny $\mu : \sigma^m E \rightarrow E$ given by

$$(x, y) \mapsto \left(-\frac{y^2}{2x^2}, \frac{\sqrt{-2}}{4} \frac{y}{x^2} (-\beta f_2 + x^2)\right),$$

showing that it is an L -curve with $K^+(\sqrt{-2})$ as a field of complete definition.

Remark 5.2 *We can also look for α, β such that $(a - b)^2 = \alpha f_1(a, b) + \beta f_2(a, b)$ and the same construction would lead to another Frey-curve.*

The definitions and properties that we use in the sequence are mainly generalizations of the work of Quer with \mathbb{Q} -curves (see [23]). For the most part the details can be found in X. Guitart thesis (see [12]).

Denote $E_{(a,b)}$ only by E . We can attach to E a 2-cocycle $c_E : G_k \times G_k \rightarrow \mathbb{Q}^*$ defined by $c_E(g, h) = \phi_g^g \phi_h \phi_{gh}^{-1}$. Let $\xi(E) \in H^2(G_k, \mathbb{Q}^*)[2]$ denote its cohomology class, K_d be a field of complete definition of E and $G = \text{Gal}(K_d/k)$. There is also an analogous cohomology class $[c_{E/K_d}] \in H^2(G, \mathbb{Q}^*)[2]$ that satisfies

$\text{Inf}_G^{G^k}[c_{E/K_d}] = \xi(E)$. Moreover, $B = \text{Res}_{K_d/k}(E/K_d)$ has endomorphism algebra isomorphic to the twisted group algebra $\mathbb{Q}^{c_{E/K_d}}[G]$ (proposition 5.32 in [12]) and B is a product of abelian varieties of GL_2 -type if and only if $\mathbb{Q}^{c_{E/K_d}}[G]$ is abelian (proposition 5.36 in [12]). If G is abelian then the algebra $\mathbb{Q}^{c_{E/K_d}}[G]$ is abelian if and only if the cocycle c_{E/K_d} is symmetric. Moreover, from the isomorphism

$$H^2(G, \mathbb{Q}^*)[2] \simeq H^2(G, \{\pm 1\}) \times \text{Hom}(G, P/P^2)$$

where $P = \mathbb{Q}^*/\{\pm 1\}$ it follows that the elements in the second factor are symmetric (because G is abelian) then c_{E/K_d} is symmetric if and only if its component in $H^2(G, \{\pm 1\})$, denoted c_{E/K_d}^\pm , is symmetric.

We now particularize to our curves. Observe that $K^+ = k(\sqrt{s})$ for some $s \in k$ and take $K_d = k(\sqrt{s}, \sqrt{-2})$ as field of complete definition of E . In this case G is abelian with generators τ and σ^m , where

$$\begin{cases} \sigma^m(\sqrt{s}) = -\sqrt{s} & \text{and} & \sigma^m(\sqrt{-2}) = -\sqrt{-2} \\ \tau(\sqrt{s}) = \sqrt{s} & \text{and} & \tau(\sqrt{-2}) = -\sqrt{-2} \end{cases}$$

The values of c_{E/K_d} were computed from the expressions of μ and $\hat{\mu}$ and can be found in Table 1. The sign component c_{E/K_d}^\pm is not symmetric and is given by the signs in the same table.

		h			
		1	τ	σ^m	$\sigma^m \tau$
g	1	1	1	1	1
	τ	1	1	-1	-1
	σ^m	1	1	-2	-2
	$\sigma^m \tau$	1	1	2	2

Table 1: Values of c_{E/K_d}

Thus we need to look for another field of complete definition K_β satisfying that c_{E/K_β} is symmetric. To achieve this we are going to use the work of Quer (see [24]) in embedding problems. A few computations shows that $c_{E/K_d}^\pm = c_{-2s, s}$ (we are using the notation in section 2 of [23]) then $\text{Inf}_G^{G^k}(c_{E/K_d}^\pm) \in H^2(G_k, \{\pm 1\})[2] \simeq \text{Br}_2(k)$ is the quaternion algebra $(-2s, s)$. At this point our aim is to apply theorem 3.1 in [24]. An application of this theorem is dependent on the value of r , nevertheless in what follows we will show that if m is odd and 2 inert in k it can be done in general. Since $r = 4m + 1$ we have $\mathbb{Q}(\sqrt{r}) \subset K^+$ and for m odd we must have $K^+(\sqrt{r})$.

Proposition 5.3 *Suppose that $r = 4m + 1$ with m odd. If 2 is inert in k then the discriminant of $(-2r, r)$ is $2r$.*

Proof: Let \mathfrak{P}_r be the prime in k above r . We can suppose that $\mathfrak{P}_r \parallel s$. If $-2rx^2 + ry^2 - z^2$ represents 0 in $k_{\mathfrak{P}_r} = \mathbb{Q}_r$ then $\mathfrak{P}_r \mid z$ and so $-2x^2 + y^2 \equiv 0 \pmod{\mathfrak{P}_r}$ hence 2 is a square modulo r . Since 2 is never a square modulo

$r = 4m + 1$ for m odd we conclude that $(-2r, r)_{\mathfrak{P}_r} = -1$. On one hand, $\iota(-2r), \iota(r)$ have opposite signals for all real places ι of L we conclude that $(-2r, r)$ is not ramified at the infinity primes. On the other hand, $(-2r, r)$ must ramify at an even number of places then the result follows. \blacksquare

Let ϵ be a character of $G_{\mathbb{Q}}$ with order 4 and conductor 2^2r thus fixing the totally real number field $K_{\epsilon} = \mathbb{Q}(\theta)$ where θ is a root of $x^4 - rx + r$. Put $k_{\epsilon} = K_{\epsilon}k$, $A = \{-2r\}$, $B = \{r\}$ and according to the notation in section 3 of [24] consider the field $K = LMN = k_{\epsilon}k(\sqrt{-2r})k$ with Galois group $G = \text{Gal}(K/k)$. Note that $k(\sqrt{r}) \subset k_{\epsilon}$ and $K_d \subset K$. Define c_{ϵ} as in [24] and $c = \theta_{\epsilon}c_{A,B}$, where $\theta_{\epsilon} = \text{Inf}_{\text{Gal}(k_{\epsilon}/k)}^G[c_{\epsilon}]$ and $c_{A,B} = \text{Inf}_{\text{Gal}(K_d/k)}^G[c_{-2s,s}]$. After identifying $\text{Inf}_G^{G^k}[\theta_{\epsilon}]$ with an element of $\text{Br}_2(k)$ we can identify it with an element in $\oplus \text{Br}_2(k_v)$ using the known exact sequence on Brauer groups

$$0 \longrightarrow \text{Br}_2(k) \longrightarrow \oplus \text{Br}_2(k_v) \longrightarrow \{\pm 1\} \longrightarrow 0$$

Now if v is a finite prime the component $(\text{Inf}_G^{G^k}[\theta_{\epsilon}])_v$ in $\text{Br}_2(k_v)$ is given by the parity of the v -component of ϵ , $\epsilon_v(-1)$. Moreover, k_{ϵ} is totally real hence $(\text{Inf}_G^{G^k}[\theta_{\epsilon}])_v = 1$ for all infinite primes v of k . Since $\epsilon_2(-1) = \epsilon_r(-1) = 1$ we have that $(\text{Inf}_G^{G^k}[\theta_{\epsilon}]) = (-2r, r)$ and the embedding problem $(K/k, \{\pm 1\}, [c])$ is unobstructed because

$$\text{Inf}_G^{G^k}[c] = (\text{Inf}_G^{G^k}[\theta_{\epsilon}]) (\text{Inf}_G^{G^k}[c_{A,B}]) = (-2r, r)(-2r, r) = 1 \in \text{Br}_2(k).$$

Now we see from theorem 3.1 in [24] that there must exists elements α_0 and α_1 in $k_{\epsilon}(\sqrt{-2})$ such that

$$\begin{aligned} N_{\sigma_0}(\alpha_0) &= -1 \\ N_{\sigma_1}(\alpha_1) &= r \\ \frac{\sigma_1 \alpha_0}{\alpha_0} &= \frac{\sigma_0 \alpha_1}{\alpha_1}. \end{aligned}$$

If δ is an element of k_{ϵ} such that $\text{Nm}_{k_{\epsilon}/k}(\delta) = -4$ we can take $\alpha_0 = \frac{\delta}{2}\sqrt{-2}$, $\alpha_1 = \sqrt{r}$. The same theorem 3.1 also gives us a splitting map β for the cocycle c . We observe that in particular $\beta_{\sigma_1} = \alpha_1/\sqrt{r} = 1$, which means that we actually have a splitting map for $[c_{\epsilon}]$. Now we pick a solution $\gamma \in k_{\epsilon}$ to the embedding problem and by construction the twisted curve E_{γ} satisfies that $c_{E_{\gamma}/k_{\epsilon}}^{\pm}$ is symmetric. Thus, as we explained before $B = \text{Res}_{k_{\epsilon}/k}(E/k_{\epsilon})$ is a product of abelian varieties of GL_2 type over k and our initial representation $\rho_{E,p}$ of G_{K^+} extends to G_k . At this point a suitable generalization of Theorem 5.12 in [22] and Theorem 5.4 in [23] would give a description of the exact decomposition of B and the character of $\rho_{E,p}$. However, we do not go further in this direction since the spaces of modular forms that we would need to apply the modular approach are already impossible to compute for $r = 13$. If $r = 5$ then $k = \mathbb{Q}$ and in joint work with L. Dieulefait we used the theory of \mathbb{Q} -curves to solve the equation $x^5 = y^5 = dz^p$ with $d = 2, 3$ for infinitely many p (see [10]).

References

- [1] N. Billerey. Critères d'irréductibilité pour les représentations des courbes elliptiques. *to appear in Intern. Journal of Number Theory*.

- [2] N. Billerey. Équations de Fermat de Type $(5, 5, p)$. *Bull. Austral. Math. Soc.*, 76(2):161–194, 2007.
- [3] N. Billerey and L. Dieulefait. Solving Fermat-type equations $x^5 + y^5 = dz^p$. *Math. Comp.*, 79:535–544, 2010.
- [4] N. Bruin. On powers as sums of two cubes. *Algorithmic number theory (edited by W. Bosma), Lecture Notes in Comput. Sci. 1838*, Springer, Berlin.
- [5] I. Chen and M. Bennett. Multi-frey \mathbb{Q} -curves and the diophantine equation $a^2 + b^6 = c^p$. <http://people.math.sfu.ca/~ichen/pub/BeCh2.pdf>.
- [6] I. Chen and S. Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322:638–656, 2009.
- [7] S. Dahmen. Classical and modular methods applied to Diophantine equations. *PhD thesis, University of Utrecht 2008, available at igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html*.
- [8] H. Darmon and A. Granville. On the equations $z^m = f(x, y)$ and $ax^p + by^q = cz^r$. *Bull. of London Math. Soc.*, 27:513–543, 1995.
- [9] L. Dieulefait and N. Freitas. Fermat-type equations of signature $(13, 13, p)$ via Hilbert cuspforms. *submitted to publication*.
- [10] L. Dieulefait and N. Freitas. The Fermat-type equations $x^5 + y^5 = 2z^p$ or $3z^p$ solved through \mathbb{Q} -curves. *submitted to publication*.
- [11] T. Gee, D. Geraghty, and T. Barnet-Lamb. Congruences between Hilbert modular forms: constructing ordinary lifts. *to appear in Duke Math Journal*.
- [12] X. Guitart. Arithmetic properties of abelian varieties under Galois conjugation. *PhD thesis, Universitat Politècnica de Catalunya, 2010* http://www-ma2.upc.es/xguitart/index_files/thesis.pdf.
- [13] F. Jarvis. Correspondences on Shimura curves and Mazur’s Principle at p . *Pacific J. Math.*, 213:267–280, 2004.
- [14] C. Khare and J.-P. Wintenberger. Serre’s modularity conjecture (i). *Inventiones Mathematicae*, 178 (3):485–504, 2009.
- [15] C. Khare and J.-P. Wintenberger. Serre’s modularity conjecture (ii). *Inventiones Mathematicae*, 178 (3):505–586, 2009.
- [16] M. Kisin. Modularity of 2-dimensional Galois representations.
- [17] A. Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta mathematica*, pages 353–386, 1968.
- [18] A. Kraus. Majorations effectives pour l’équation de Fermat généralisée. *Canad. J. Math*, 49:no. 6 1139–1161, 1997.
- [19] A. Kraus. Sur l’équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7:1–13, 1998.

- [20] A. Kraus. On the Equation $x^p + y^q = z^r$: A Survey. *The Ramanujan Journal*, 3:315–335, 1999.
- [21] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *Journal of Number Theory*, 44:119–152, 1993.
- [22] E. E. Pyle. Abelian varieties over \mathbb{Q} with large endomorphisms algebras and their simple components over \mathbb{Q} . *Progress in Mathematics*, 224:189–234, 2004.
- [23] J. Quer. \mathbb{Q} -curves and Abelian varieties of GL_2 -type. *Proc. London Math. Soc.*, (3) 81:285–317, 2000.
- [24] J. Quer. Embedding problems over abelian groups and an application to elliptic curves. *J. Algebra*, 237:186–202, 2001.
- [25] A. Rajaei. On the levels of mod Hilbert modular forms. *J. reine angew.*, 537:33–65, 2001.
- [26] C. Skinner and A. Wiles. Residually reducible representations and modular forms. *Publ. Math. IHES*, 89:5–126, 2000.
- [27] A. Wiles. Modular elliptic curves and Fermat’s Last Theorem.